NASA Procedural Requirements

NPR 1382.1A
Effective Date: July 10, 2013
Expiration Date: July 10, 2018

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Privacy Procedural Requirements

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | AppendixA | AppendixB | AppendixC | AppedixD | AppendixE | ALL |

Appendix A: Definitions

Information in Identifiable Form (IIF). In accordance with section 208(d) of the e-Gov act, IIF is defined as "... any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

In accordance with OMB Memorandum M-03-22, IIF "... is information in an IT system or online collection: (i) that directly identifies an individual (e.g. name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance, for additional information on IIF.

Non-Sensitive Personally Identifiable Information (PII). Non-Sensitive PII is information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

Member of the Public. Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance for the distinction of member of the public as it pertains to e-Gov and the PRA.

Personally Identifiable Information (PII). In accordance with M-07-16, PII "... refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

In accordance with M-10-23, "... [t]he definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual."

For purposes of NASA policy, sensitive PII excludes personal information collected and or maintained by NASA employees and contractors for personal rather than NASA business purposes, as allowed under NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology. Examples of such excluded data include contact information for family, relatives, and doctors.

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance, for additional information on PII.

Privacy Impact Assessment (PIA). In accordance with M-03-22, a PIA "... is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

Refer to ITS-HBK-1382.03, Privacy Risk Management and Compliance for additional information on PIAs.

Privacy Breach. A privacy breach is also known as an "incident." An incident is any adverse event or situation associated with any information collection containing PII that poses a threat to integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information. Refer to ITS-HBK-1382.05, Privacy Incident Response and Management, for specific information on privacy breach.

Sensitive Personally Identifiable Information. This definition is related to incident reporting only as outlined in Chapter 5 of this NPR. All PII, regardless of whether it is sensitive or non-sensitive, shall be protected as outlined in this NPR and as defined in OMB Memorandum M-07-16.

Sensitive PII is a combination of PII elements, which if lost, compromised, or disclosed without authorization could be used to inflict substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Refer to ITS-HBK-1382.05, Privacy Incident Response and Management, for the distinction of sensitive versus non-sensitive PII.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | AppendixA | AppendixB | AppendixC | AppedixD | AppendixE | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS